Listing of Claims:

1. (Currently Amended) A method, comprising:

sending a Process Login (PLOGI) message to a target entity, wherein the PLOGI process allows a source entity and the target entity to determine that an authentication message has a length that exceeds an authentication message length supported by the target entity in a fibre channel Fabric;

fragmenting the authentication message into message fragments including a first message fragment and a second message fragment;

generating a first Extended Link Services (ELS) message including the first message fragment, wherein the first ELS message is associated with a first exchange;

generating a second ELS message including the second message fragment, wherein the second ELS message is associated with a second exchange;

identifying each fragment with a one-bit sequence number, wherein the target entity accepts a fragment if the sequence number bit differs from the previous fragment and rejects the fragment if the sequence number bit matches the previous fragment;

sending the message fragments including the first message fragment and the second message fragment to the target entity, wherein the second message fragment is sent after determining that the first exchange is complete.

2. (Original) The method of claim 1, wherein fragmenting the authentication message into message fragments further comprises setting a fragmentation bit in each message fragment except the last message fragment.

3. (Original) The method of claim 2, wherein the setting of the fragmentation bit of one of the message fragments indicates that a subsequent message fragment is to be sent.

4. (Original) The method of claim 1, wherein fragmenting the authentication message into message fragments further comprises resetting a fragmentation bit in the last message fragment of the authentication message.

5. (Original) The method of claim 1, wherein fragmenting the authentication message into message fragments further comprises labeling each message fragment with a Sequence Number.

6. (Original) The method of claim 4, wherein the resetting of the fragmentation bit in the fragmentation field of the last message fragment indicates that no subsequent message fragments will follow the last message fragment.

7. (Original) The method of claim 1, wherein the message comprises, but is not limited to, authentication information and contains one or more of the following fields:

a field that identifies the authentication message as an authentication message; and

an authentication command code field that identifies the particular authentication message of an authentication protocol.

8. (Original) The method of claim 6, wherein the authentication protocol comprises but is not limited to the following protocols: DH-CHAP, SRP, or FCAP.

9. (Original) The method of claim 1, wherein the target entity is an end device in the Fabric.

10. (Original) The method of claim 1, wherein the target entity is the Fabric.

11. (Original) The method of claim 6, wherein the target entity either accepts or discards the message fragment based on the value of the Sequence Number.

12-23. (Canceled)

24. (Currently Amended) An apparatus, comprising:

a processor operable to determine that an authentication message has a length that exceeds the message length supported by a target entity in a fibre channel Fabric, wherein the processor makes this determination ~~during~~ after sending a Process Login (PLOGI) message to a target entity, wherein the PLOGI process allows a source entity and the target entity, wherein the processor is further operable to fragment the authentication message into message fragments including a first message fragment and a second message fragment, and generate a first Extended Link Services (ELS) message including the first message fragment and a second ELS message including the second message fragment, wherein the first ELS message is associated with a first exchange and the second ELS message is associated with a second exchange, and identify each fragment with a one-bit sequence number, wherein the target entity accepts a fragment if the sequence number bit differs from the previous fragment and rejects the fragment if the sequence number bit matches the previous fragment;

an interface connected to the processor, the interface operable to send the message fragments including the first message fragment and the second message fragment to the target entity, wherein the second message fragment is sent after determining that the first exchange is complete.

25. (Previously Presented) The apparatus of claim 24, wherein the processor sets a fragmentation bit in each message fragment except the last message fragment.

26. (Previously Presented) The apparatus of claim 25, wherein the fragmentation bit is used to indicate that a subsequent message fragment is to be sent by the initiating entity.

27. (Previously Presented) The apparatus of claim 24, wherein a fragmentation bit in the last message fragment of the authentication message is set.

28. (Previously Presented) The apparatus of claim 24, wherein each message fragment is labeled with a Sequence Number.

29. (Currently Amended) A system, comprising:

means for sending a Process Login (PLOGI) message to a target entity, wherein the PLOGI process allows a source entity and the target entity to determine that an authentication message has a length that exceeds an authentication message length supported by the ~~a~~ target entity in a fibre channel Fabric;

means for fragmenting the authentication message into message fragments including a first message fragment and a second message fragment;

means for generating a first Extended Link Services (ELS) message including the first message fragment, wherein the first ELS message is associated with a first exchange;

means for generating a second ELS message including the second message fragment, wherein the second ELS message is associated with a second exchange;

means for identifying each fragment with a one-bit sequence number, wherein the target entity accepts a fragment if the sequence number bit differs from the previous fragment and rejects the fragment if the sequence number bit matches the previous fragment;

means for sending the message fragments including the first message fragment and the second message fragment to the target entity, wherein the second message fragment is sent after determining that the first exchange is complete.

30. (Previously Presented) The system of claim 29, wherein fragmenting the authentication message into message fragments further comprises setting a fragmentation bit in each message fragment except the last message fragment.

31. (Previously Presented) The system of claim 30, wherein the setting of the fragmentation bit of one of the message fragments indicates that a subsequent message fragment is to be sent.

32. (Previously Presented) The system of claim 29, wherein fragmenting the authentication message into message fragments further comprises resetting a fragmentation bit in the last message fragment of the authentication message.

33. (Previously Presented) The system of claim 29, wherein fragmenting the authentication message into message fragments further comprises labeling each message fragment with a Sequence Number.

34. (Previously Presented) The system of claim 32, wherein the resetting of the fragmentation bit in the fragmentation field of the last message fragment indicates that no subsequent message fragments will follow the last message fragment.

35. (Previously Presented) The system of claim 29, wherein the message comprises, but is not limited to, authentication information and contains one or more of the following fields:

a field that identifies the authentication message as an authentication message; and

an authentication command code field that identifies the particular authentication message of an authentication protocol.

36. (Previously Presented) The system of claim 29, further comprising means for sending an RPBC (Report Port Buffer Conditions) message to the target entity, wherein the target entity responds with information regarding a maximum authentication message length supported by the target entity.

37. (Previously Presented) The system of claim 36, further comprising means for sending information regarding a maximum authentication message length supported by the source entity.